Um Esquema Cooperativo para Análise da Presença de Ataques EUP em Redes Ad Hoc de Rádio Cognitivo

Julio Soto, Saulo Queiroz*, Michele Nogueira

[1]NR2 – Núcleo de Redes sem Fio e Redes Avançadas
Universidade Federal do Paraná (UFPR), Brasil

{jchsoto, sjbqueiroz, michele}@inf.ufpr.br

Abstract. *In Cognitive Radio Ad Hoc Networks, malicious Secondary Users can exploit CR capabilities to perform Primary User Emulation Attacks (PUEA). These attacks pretend the characteristics of a Primary User, giving to malicious users the priority of using licensed frequencies over well-behaved unlicensed Secondary Users. To address this problem, studies in the literature have proposed the use of specific criteria to detect PUE attacks. Such solutions, however, do not consider the use of multiple different criteria to infer the presence of PUEA on the network. To fill this gap, we propose INCA, a novel multIple criteria scheme for the deceNtralized and Cooperative Analysis of the PUEA presence in CRAHNs. INCA follows two phases. On the first, each SU employs multiple criteria to define a hypothesis about the potential existence of attacks; whereas on the second, these hypotheses are exchanged among neighbors, and each SU employs the Bayes theorem to calculate the final probability of the PUEA presence. Simulation results show the improvement and effectiveness of the multi-criteria approach.*

Resumo. *Nas redes ad hoc de rádio cognitivo, os usuários mal intencionados podem tirar proveito das funcionalidades da tecnologia de rádio cognitivo para realizar ataques de emulação de usuário primário (EUP). Nestes ataques, os usuários mal intencionados imitam as características dos usuários licenciados, visando obter prioridade no uso das bandas de radiofrequências licenciadas e ameaçando o funcionamento da rede. A fim de tratar deste problema, trabalhos na literatura utilizam critérios específicos para detecção de ataques EUP. Tais soluções, contudo, não consideram conjuntamente o uso de múltiplos e diferentes critérios que enriquecem o consenso de inferência sobre a presença de um ataque EUP na rede. Diante deste contexto, este trabalho apresenta INCA, um esquema de múltIplos critérios para aNálise Cooperativa da presença de Ataques EUP em redes ad hoc de rádio cognitivo. O esquema INCA é composto por duas fases. Na primeira, cada usuário não licenciado emprega múltiplos critérios para definir uma hipótese individual da presença dos ataques EUP. Na segunda, essas hipóteses são trocadas entre os seus vizinhos e cada usuário não licenciado calcula a probabilidade final da presença de um ataque EUP através do teorema de Bayes. Os resultados de simulação mostram a melhoria e a eficácia da cooperatividade e do uso de múltiplos critérios quando aplicados simultaneamente.*

*autor também filiado à UTFPR (Universidade Tecnológica Federal do Paraná), Brasil.

1. Introdução

A tecnologia de rádio cognitivo (RC) permite o surgimento das redes ad hoc de rádio cognitivo (do inglês *Cognitive Radio Ad Hoc Network - CRAHN*), nas quais os usuários secundários não licenciados (US) podem aproveitar oportunisticamente as bandas de radiofrequências licenciadas e subutilizadas pelos usuários primários (UPs) (estas bandas também são chamadas de *espaços em branco* ou *ociosos*). As CRAHNs podem ser aplicadas a diferentes situações, como aquelas de emergência, desastres naturais, conflitos bélicos, se beneficiando do uso de espaços em branco existentes, independente da localização do USs [Akyildiz et al. 2009]. Em uma CRAHN, os USs são capazes de comunicar-se entre eles através de múltiplos saltos. Para isto, inicialmente um US realiza um *sensoreamento* do espectro a fim de identificar os espaços em branco, seguido de uma *decisão* sobre qual espaço ocioso ele reutilizará para ter acesso ao espectro. Tal processo não pode causar qualquer interferência ao UP. Dessa forma, mediante a presença de um UP, o US deve eleger uma outra banda e realizar um *salto* de frequência para liberar a faixa atual. Durante todo este processo um US pode sofrer interrupções temporais até que um novo canal disponível seja encontrado [Mitola and Maguire 1999, Akyildiz et al. 2008, Lee and Akyldiz 2011].

As CRAHNs melhoram a eficiência no uso do espectro devido à utilização oportunista dos espaços em branco [Felice et al. 2011]. Por outro lado, tal característica vem sendo explorada como uma *nova* falha de segurança em redes sem fio. Um clássico exemplo nesse sentido é o ataque de emulação de usuário primário (EUP) e suas variantes [Tan et al. 2011, Chen and Park 2006]. Em geral, o ataque EUP é gerado por um US mal intencionado que tenta maximizar seu próprio uso do espectro, denominado US egoísta, ou gerar uma negação do serviço (*DoS* do inglês *Denial of Service*), denominado US malicioso. Um US mal intencionado (atacante) manipula suas configurações de rádio para imitar o comportamento de um UP. Assim, ele prejudica a oportunidade de acesso ao espectro de um US legítimo.

Criar soluções para detectar ou mitigar o efeito de USs mal intencionados constitui um desafio para a segurança dessas redes, devido à dificuldade em proteger a rede contra esses ataques e ao fato deles comprometerem severamente o desempenho dos US legítimos em perdas de oportunidades de acesso ao espectro [Chen and Park 2006, Chen et al. 2008, Jin et al. 2009, Jin et al. 2010]. Nesse sentido, os trabalhos na literatura para detecção ou mitigação desses ataques seguem enfoques (*descentralizadas* ou *centralizadas*) com abordagens *cooperativas* ou *não-cooperativas*. No entanto, esses trabalhos concentram uma grande parte do seu foco na definição do tipo de abordagens que irão utilizar, deixando outro aspecto muito importante de lado: a definição dos **critérios** para decidir sobre a presença de ataques EUP. O uso conjunto de diferentes critérios representam um foco importante devido ao fato de enriquecer as análises com múltiplos dados a fim de chegar a um consenso de inferência sobre a presença ameaçadora de atacantes na rede. Por outro lado, até onde sabemos, nenhum dos trabalhos na literatura aborda a concepção de um esquema de múltiplos critérios para detectar a presença de ataque EUP.

Assim, para tratar deste problema, nós propomos INCA, um esquema de múlt**I**plos critérios para a**N**álise **C**ooperativa da presença de **A**taques EUP em redes ad hoc de rádio cognitivo. O esquema INCA consiste de duas fases: **individual** e **cooperativa**. Na primeira fase, cada US realiza uma coleta de informação do meio, esta é realizada

mediante a função de sensoreamento do espectro aplicando a técnica de detecção pela energia. Esta técnica foi escolhida por não precisar de um conhecimento prévio do sinal e pelo seu baixo custo computacional ao comparar com outras técnicas existentes (ex. [Arianandа et al. 2009, Fragkiadakis et al. 2012]). Após o sensoreamento do espectro, cada US utiliza múltiplos critérios para determinar uma probabilidade preliminar da presença de ataque EUP. Na segunda fase, os USs trocam hipóteses preliminares de detecção entre si. Em seguida, cada US aplica o teorema de Bayes sobre as probabilidades preliminares coletadas, a fim de calcular a probabilidade final da presença de ataques EUPs. A aplicação do teorema de Bayes permite a um nó atualizar sua probabilidade acerca da presença de um ataque na rede a partir do conhecimento das probabilidades de ataque advindas dos seus vizinhos. Este cálculo final determina a presença de um ou mais USs mal intencionados atacando a CRAHN. Resultados de simulações mostram que o esquema INCA melhora a análise probabilística da presença de ataque EUP em todos os cenários avaliados, sobretudo quando as duas fases do esquema são executadas. Estes resultados fortalecem o argumento de utilização de múltiplos critérios na detecção de ataques EUP.

Este trabalho está organizado da seguinte forma. Na Seção 2 descrevemos os trabalhos relacionados. Na Seção 3, nós apresentamos uma explicação sobre os ataques EUPs. Na Seção 4, nós detalhamos o esquema INCA como proposta para determinar a presença dos ataques EUP nas CRAHNs. Na Seção 5, avaliamos o esquema diante de diferentes cenários e descrevemos os resultados obtidos. Finalmente, na Seção 6, apresentamos as conclusões do artigo e os trabalhos futuros.

2. Trabalhos relacionados

Apesar de ser um tópico de pesquisa recente, trabalhos na literatura vêm empregando diferentes estratégias na tentativa de detectar os ataques EUP nas CRAHN. Neste contexto, observamos que os esquemas de detecção de ataques EUP vêm evoluindo no uso de abordagens centralizadas não-cooperativas a abordagens descentralizadas cooperativas. As primeiras soluções apresentavam modelos centralizados não-cooperativos para a detecção de ataques EUP. Uma primeira abordagem é vista em [Chen and Park 2006], utilizando duas técnicas baseadas na recepção do sinal e na localização dos transmissores. Em [Chen et al. 2008], a técnica LocDef é utilizada, tendo como base a localização do transmissor. Em [Li and Han 2010], o esquema Dogfight, é apresentado e tem como referência a competição entre o atacante e US legítimo utilizando a teoria de jogos. Por outro lado, uma das principais limitações nestes tipos de abordagens é a forte possibilidade de sobrecarregar a estação base central, além de poderem sofrer com altos níveis de latência.

Similarmente, esquemas baseados em abordagens centralizadas cooperativas foram propostos. Em [Min et al. 2011], utiliza-se a USs como sensores para descoberta dos atacantes na rede a partir da transmissão do UP. O esquema denominado IRIS [Chen et al. 2011] tem como base a potência de recepção combinada com pesos de importância de acordo com o estado do canal monitorado pelo US. Por outro lado, [Jin et al. 2010] apresenta um esquema baseado na utilização de uma aproximação log-normal para caracterizar a potência de recepção em cada nó e chegar a um consenso entre as informações coletadas pelos nós em uma estação base central a fim de determinar a probabilidade da presença do ataque EUP. No entanto, estes esquemas podem resolver

os problemas das abordagens centralizadas não-cooperativas, mas apresentam outro problema, a alta taxa de falsos negativos e positivos.

Para reduzir as limitações das abordagens centralizadas cooperativas surgiram as abordagens distribuídas cooperativas, as quais seguem diferentes esquemas de detecção ou mitigação de ataques EUP. Em [Yuan et al. 2011], um esquema baseado na propagação de confianças foi proposto (do inglês *belief propagation - BP*). Este esquema calcula a força do sinal recebido por cada nó, e depois troca informação com os vizinhos a fim de determinar a presença do atacante. Em [Z. Jin and Subbalakshmi 2010], um esquema chamado NEAT foi apresentado. Ele utiliza uma aproximação log-normal para caracterizar a potência de recepção e determinar a presença dos atacantes com base na informação da vizinhança do nó monitor. No entanto, todas estas abordagens e esquemas existentes realizam uma análise da presença de ataque EUP na rede considerando apenas um ou dois critérios. Neste trabalho defendemos o uso de um esquema capaz de lidar com múltiplos critérios em abordagens distribuídas e cooperativas a fim de melhorar da taxa de detecção de ataques EUP nas CRAHNs.

3. Ataque de emulação de usuário primário

O ataque EUP foi apresentado por [Chen and Park 2006]. Este ataque é gerado por um US mal intencionado que manipula os parâmetros de configuração de seu rádio para fingir ser um UP [Jin et al. 2009, Chen et al. 2008]. Isto é possível pela capacidade e facilidade de configuração dos dispositivos equipados com RC. Um US mal intencionado pode alterar os parâmetros de seu dispositivo de rádio para imitar as características (ex. potência de transmissão, o tipo de modulação, a frequência utilizada, a largura de banda, a taxa de transmissão) de um UP. Como consequência, o atacante pode reduzir o número de espaços em branco disponíveis no espectro, gerando um *DoS*, e prejudicando seriamente o acesso ao espectro dos USs legítimos [Jin et al. 2009].

No ataque EUP, o atacante pode ser classificado em dois tipos: (i) um **usuário malicioso**, que imita o comportamento do UP para afetar o desempenho da rede, e (ii) um **usuário egoísta**, que também imita o comportamento de um UP a fim de obter as vantagens de prioridade de uso do espectro atribuído a ele [Chen and Park 2006]. Os dois tipos de ataque EUP afetam diretamente o processo de compartilhamento do espectro e reduzem drasticamente os recursos disponíveis aos demais USs legítimos [Chen et al. 2008]. Desta forma não fazemos distinção entre os dois tipos de ataques EUP neste trabalho.

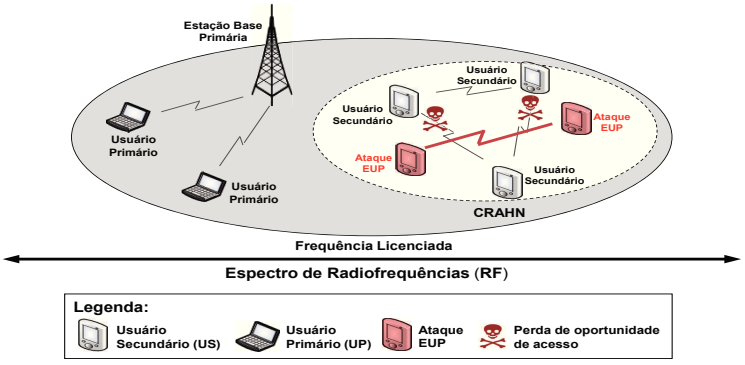

Figura 1. CRAHN sob ataque EUP

A Figura 1 ilustra um US legítimo utilizando oportunisticamente o espectro ocioso. Em primeiro lugar, o US realiza o sensoreamento do espectro e após acessa as frequências ociosas. Sempre que um UP inicia atividade em sua banda licenciada, o US move-se para outra frequência ociosa do espectro. No entanto, os ataques EUPs podem comprometer diferentes faixas de frequências, levando os espaços em branco a serem ocupados. Desta forma, os US legítimos perdem a oportunidade de acessar o espectro, pois detectam a atividade dos atacantes como sendo atividades de UPs legítimos.

4. Esquema INCA

Nesta seção descrevemos o esquema INCA proposto, seguindo suas duas fases, **individual** ou e de **cooperação**, conforme ilustradas na Figura 2. Em síntese, na primeira fase, simplesmente denotada por A, cada US considera múltiplos critérios associados a pesos de importância específicos para determinar uma *probabilidade preliminar* $P_{n_i}(A)$ de acontecer um ataque detectável pelo nó n_i. Da perspectiva de n_i, $P_{n_i}(A)$ é apenas uma estimativa inicial sobre a presença do ataque EUP na rede. Em seguida, a fase de cooperação (denotada por B), é caracterizada pela recepção de informações de probabilidades oriundas de nós vizinhos. Dessa forma, cada vizinho n_j compartilhará sua respectiva probabilidade preliminar (denotada por $P_{n_j}(B)$) com o nó n_i. Por fim, o esquema INCA emprega o teorema de Bayes para que o nó n_i possa calcular sua probabilidade final $P_{n_i}(A|B)$ a partir de $P_{n_i}(A)$ e das informações de probabilidades recebidas de seus vizinhos.

Nas próximas seções, consideramos a notação sumarizada na Tabela 1 para explicar melhor essas fases. N_{UP} representa o conjunto de usuários primários, e N_S expressa o conjunto de usuários secundários (nós), onde n_i representa um US arbitrário na rede ad hoc de rádio cognitivo. Por sua vez, $N_S = N_{SL} \cup N_{SB}$, em que N_{SL} é o subconjunto de USs legítimos e N_{SB} é o subconjunto de US mal intencionados. c expressa o número de critérios considerados para a análise da presença do ataque EUP e $P_{n_i}(A)$ é a probabilidade preliminar do i-ésimo US na rede, isto é $1 \leq n_i \leq |N_{SL}|$.

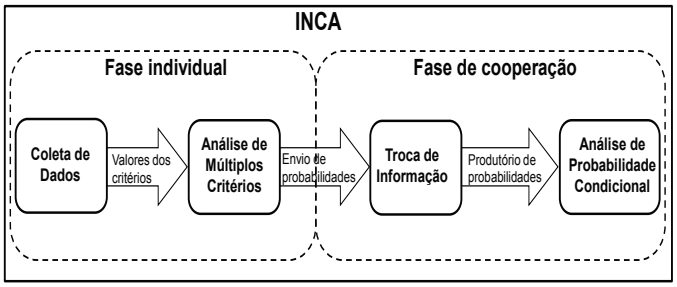

Figura 2. Esquema INCA

4.1. Fase individual

Na primeira fase do esquema INCA, o i-ésimo US realiza uma coleta de dados do meio. Esta coleta é realizada por uma técnica de sensoreamento do espectro definida na tecnologia de RC. Particularmente neste trabalho, utilizamos a técnica de detecção de sinal pela energia [Zhang et al. 2009, Subhedar and Birajdar 2011] devido a sua simplicidade de implementação e baixo custo computacional como demonstrado por

Tabela 1. Notação do esquema INCA

Notação	Definição
N_{UP}	Conjunto de usuários primários
N_{SL}	Conjunto de usuários secundários legítimos
N_{SB}	Conjunto de usuários secundários mal intencionados
N_S	Conjunto de usuários secundários
n_i	i-ésimo usuário secundário arbitrário
n_j	j-ésimo usuário secundário vizinho de n_i
$P_{n_i}(A)$	Probabilidade preliminar calculada pelo nó n_i
$P_{n_j}(B)$	Probabilidade preliminar calculada pelo vizinho n_j
$P_{n_i}(A\|B)$	Probabilidade final calculada pelo nó n_i
$P_{n_j}(B\|A)$	Probabilidade final calculada pelo vizinho n_j
$\mathcal{S}$	Conjunto de critérios
$\mathcal{W}$	Conjunto de pesos de importância para os critérios
$\mathcal{MIN}$ e $\mathcal{MAX}$	Conjunto de valores mínimos e máximos dos critérios

[Arianandа et al. 2009, Fragkiadakis et al. 2012]. Após a coleta de dados, estes dados são agrupados em um conjunto de critérios estabelecido pelo esquema INCA.

Em seguida, o i-ésimo US calcula $P_{n_i}(A)$ sobre os conjuntos $\mathcal{S}$, $\mathcal{W}$, $\mathcal{MIN}$ e $\mathcal{MAX}$. Todo este processo é realizado pelo método de análise de múltiplos critérios NWAUF (do inglês *Normalized Weighted Additive Utility Function*) [Malakooti et al. 2006], pois estudos mostram o baixo custo computacional deste método em comparação a outros para análise de múltiplos critérios, como o AHP (*Analytic Hierarchy Process*) [Saaty 1980] ou ELECTRE [Benayoun et al. 1966], e as suas respectivas variantes [Malakooti et al. 2006, Wang and Triantaphyllou 2008]. Os passos gerais do método são apresentados no Algoritmo 1. $\mathcal{S}$ representa o conjunto de amostras coletadas para cada um dos critérios. Os conjuntos $\mathcal{MIN}$ e $\mathcal{MAX}$ são compostos pelos valores mínimos e máximos para cada um dos $|\mathcal{S}|$ critérios. Estes conjuntos são usados pelo algoritmo NWAUF para normalizar os valores em $\mathcal{S}$ e gerar o conjunto normalizado correspondente $\overline{\mathcal{S}} = \{\overline{s} \mid 0 \leq \overline{s} \leq 1\}$ (linhas 5–6). Finalmente, o algoritmo utiliza o conjunto de pesos $\mathcal{W} = \{w_1, w_2, \ldots, w_c \mid \sum_{z=1}^{c} w_z = 1\}$, em que cada peso de importância é atribuído a um critério em $\overline{\mathcal{S}}$ para calcular $P_{n_i}(A)$ (probablidade preliminar do i-ésimo US) (linha 7).

Algoritmo 1 Análise NWAUF

1: **procedimento** NWAUFANALYSIS($\mathcal{S}, \mathcal{W}, \mathcal{MIN}, \mathcal{MAX}$)
2: $P_{n_i}(A) \leftarrow 0$;
3: $\overline{\mathcal{S}} \leftarrow \emptyset$;
4: **para todo** $z = 1 \rightarrow |\mathcal{S}|$ **faça**
5: $\overline{s_z} \leftarrow \dfrac{\mathcal{S}_z - \mathcal{MIN}_z}{\mathcal{MAX}_z - \mathcal{MIN}_z}$;
6: $\overline{\mathcal{S}} \leftarrow \overline{\mathcal{S}} \cup \{\overline{s}\}$;
7: $P_{n_i}(A) \leftarrow P_{n_i}(A) + W_z \cdot \overline{s}_z$;
8: **fim para**
9: **fim procedimento**

Cada nó aplica o método NWAUF para calcular uma probabilidade preliminar da presença do ataque EUP através da agregação de dados de múltiplos critérios. Tal resultado é então utilizado para tomar a decisão final na fase de cooperação do INCA. A

Figura 3 destaca cada passo da análise NWAUF de múltiplos critérios na primeira fase do INCA.

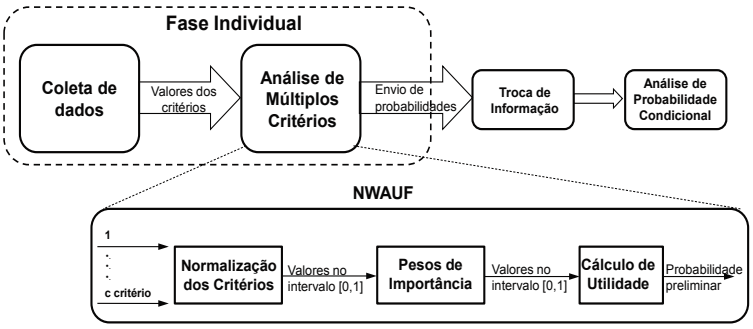

Figura 3. Fase individual do INCA

4.2. Fase de cooperação

Na fase de cooperação, o i-ésimo US não só realiza o compartilhamento de $P_{n_i}(A)$ (probabilidade preliminar da presença de ataque EUP), mas também recebe as probabilidades preliminares de outros nós vizinhos. O esquema INCA considera como vizinhos, os USs que estão no mesmo canal de frequência a um salto de distância de um nó. Esta troca de informação é realizada estabelecendo um canal de transmissão comum entre o US e cada um de seus vizinhos. A informação é colocada em um pacote de controle e enviada aos vizinhos, desta mesma forma os vizinhos ao receber o pacote, eles retornam um pacote de controle contendo suas probabilidades preliminares de detecção.

Depois de receber $k \leq |N_{SL}| - |\{n_i\}|$ probabilidades preliminares de sua vizinhança, o nó $n_i \in N_{SL}$ calcula sua probabilidade final $P_{n_i}(A|B)$ referente à presença de um ataque EUP na rede por meio do teorema de Bayes (Eq. 1). Este teorema permite calcular a probabilidade condicionada $P(A|B)$ de acontecer um dado evento A, mediante a ocorrência de um evento B. Para isso, o teorema considera uma probabilidade preliminar $P(A)$ de acontecer um evento A sem a influência do evento B. Além disso ele também considera a probabilidade preliminar $P(B)$ de acontecer o evento B bem como a probabilidade inversa de $P(A|B)$, isto é, $P(B|A)$.

Neste contexto utilizamos o teorema de Bayes para calcular a probabilidade final $P_{n_i}(A|B)$ do nó n_i a partir dos valores das probabilidades $P_{n_i}(A)$, $P_{n_j}(B)$ e $P_{n_j}(B|A)$. Em particular, o evento A denota o acontecimento de um ataque EUP da perspectiva do nó n_i. A probabilidade $P_{n_i}(A)$ é inicialmente estimada por n_i a partir do método NWAUF, como explicado na fase individual do esquema INCA. Do mesmo modo, cada vizinho do nó n_i calcula sua respectiva probabilidade preliminar acerca de um ataque EUP na rede. Da perspectiva do nó n_i, o evento B denota o recebimento de estimativas de probabilidade de ataque de seus vizinhos n_j, $j = 1, \ldots, k$, em que k é o total de vizinhos do nó n_i. Cada vizinho n_j calcula sua própria probabilidade preliminar acerca de um ataque EUP na rede que são denotadas por $P_{n_j}(B)$ da perspectiva do nó n_i.

O teorema de Bayes requer que cada probabilidade do tipo $P_{n_j}(B|A)$ (i.e., probabilidade final de vizinhos) seja estimada para o cálculo da *primeira* amostra de probabilidade final $P_{n_i}(A|B)$ de um dado nó n_i. Em particular para nosso esquema, este valor

foi inicialmente definido em 0.5. Note (da eq. 1), contudo, que o fato de definirmos um mesmo valor constante para toda probabilidade do tipo $P(B|A)$ implica que a primeira amostra de uma probabilidade do tipo $P(A|B)$ seja inteiramente influenciada apenas por valores oriundos de medições, isto é, probabilidades dos tipos $P(A)$ e $P(B)$. Dessa forma, os valores das probabilidades do tipo $P(B|A)$ serão conhecidos para o cálculo das demais amostras de probabilidades do tipo $P(A|B)$ através da etapa de compartilhamento do esquema INCA.

A Figura 4 destaca os passos para que cada US determine a probabilidade da presença do ataque EUP através da probabilidade condicional definida pelo teorema de Bayes.

$$P_{n_i}(A|B) = \frac{P_{n_i}(A).P_{n_1}(B|A)}{[\sum_{j=1}^{k} P_{n_j}(B).P_{n_j}(B|A)]} \quad (1)$$

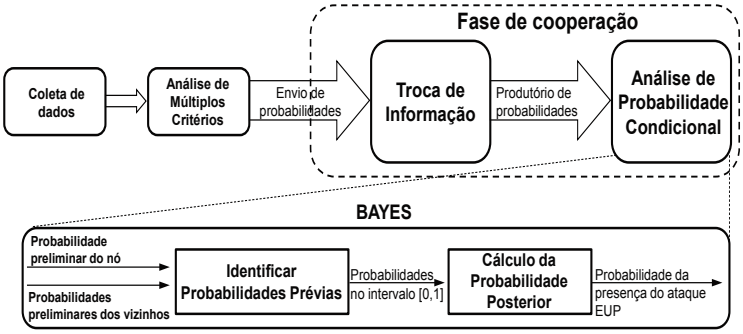

Figura 4. Fase de cooperação do INCA

4.3. INCA - Estudo de caso

O esquema INCA foi projetado para suportar múltiplos critérios a fim de analisar a presença de ataques EUP. Sem perda de generalidade, nesta subseção, nós selecionamos três critérios a fim de verificar o esquema INCA através de um estudo de caso. Os critérios escolhidos para análise do esquema INCA são a *intensidade do sinal recebido*, *potência de transmissão* e a *distância* com pesos de 50%, 25% e 25%, respectivamente. Conforme reportamos na seção 5.2, tais pesos representam pelo menos uma configuração que demonstra a melhoria fornecida pela abordagem de múltiplos critérios proposta frente à abordagem representante do estado da arte. Esse resultado constitui o foco chave deste trabalho. Em face disso, o desenvolvimento de algoritmos que exploram a melhor configuração de pesos de forma *on-line* demanda um estudo particular que deixamos para trabalhos futuros.

A primeira fase do esquema INCA requer que os valores das métricas escolhidas possam ser amostrados. No contexto do nosso estudo de caso, a metodologia de amostragem para valores de intensidade do sinal demanda explanação adicional haja visto tal métrica ser intrinsecamente dependente do método de sensoriamento de espectro necessário aos nós com capacidade de rádio cognitivo, conforme discutimos a seguir.

A intensidade do sinal percebida por US legítimo $n_i \in N_{SL}$ a partir de um nó arbitrário $n_j \in N - \{n_i\}$ em um instante t é denotado por $P_R^{n_j \to n_i}(t)$. A potência de transmissão de n_j é denotada por $P_T^{n_j}(t)$ e a distância entre eles é $d_{n_j}^{n_i}(t)$.

$$y_{n_i}(t) = \begin{cases} \eta(t), & H_0 \\ P_R^{n_j \to n_i}(t) + \eta(t), & H_1 \end{cases} \quad (2)$$

Levando em conta os modelos relacionados para o critério $P_R^{n_j \to n_i}(t)$, a primeira consideração a ser feita diz respeito a uma transmissão estar ocorrendo no espectro licenciado ou não, isto é, se o nó n_i deve detectar o espectro para diferenciar o ruído da transmissão real. Conforme a Eq. 2 da técnica de detecção de atividade de espectro baseada em energia, a hipótese H_1 expressa que um nó arbitrário n_j está usando o espectro licenciado. Neste caso, a potência total $y_{n_i}(t)$ percebida pelo n_i no instante t é $P_R^{n_j \to n_i}(t)$. Adicionalmente, assumimos que o canal é perturbado por um ruído aditivo Gaussiano branco $\eta(t)$. A hipótese H_0 ocorre quando não é realizada nenhuma transmissão no espectro e apenas o ruído pode ser detectado, ou seja, $P_R^{n_j \to n_i}(t) = 0$.

Por sua vez, INCA obtém $P_R^{n_j \to n_i}(t)$ a partir de $P_T^{n_j}(t)$ e $d_{n_j}^{n_i}(t)$ por meio dos modelos de propagação de rádio descritos na Eq. 3. Em particular, nós assumimos o modelo de propagação *Free-Space* para o sinal detectado por n_i se $n_j \in N_{UP}$, e o modelo de propagação *two ray ground* para o sinal detectado por n_i a partir de um usuário não primário i.e., US mal intencionado ou um US legítimo ([Z. Jin and Subbalakshmi 2010, Anand et al. 2008]). Finalmente, G_p^2 e G_s^2 representam os fatores de dissipação log-normais para os respectivos modelos supracitados.

$$P_R^{n_j \to n_i}(t) = \begin{cases} P_T^{n_j}(t)(d_{n_j}^{n_i}(t))^{-2} G_p^2, \text{ se } n_j \in N_P \\ P_T^{n_j}(t)(d_{n_j}^{n_i}(t))^{-4} G_s^2, \text{ se } n_j \in N_S \end{cases} \quad (3)$$

5. Análise e avaliação

Nesta seção, são descritos os cenários de simulação usados para avaliar o desempenho do esquema INCA. Inicialmente, são apresentados o ambiente de simulação, os parâmetros e suas justificativas. Em seguida, os resultados e análises.

5.1. Cenários de simulação

Nossas simulações estão compostas de $|N_{UP}| = 2$ e $|N_S| = 50$ nós estáticos, onde a quantidade de $|N_{SL}|$ e $|N_{SB}|$ variam para refletir diferentes taxas de atacantes na rede. Sempre que um US pretende transmitir, ele executa uma função de sensoreamento pela energia do sinal para detectar um canal ocioso. Além disso, cada UP acessa a sua banda licenciada seguindo uma distribuição aleatória. Por sua vez, assumimos que os atacantes acessam (i.e. atacam) o canal conforme uma distribuição uniforme.

Na rede, um usuário primário $UP \in N_{UP}$ emprega seu canal licenciado para realizar uma transmissão primária. A potência de transmissão $P_T^{UP}(t)$ de UP pode ser facilmente determinada pelo padrão operacional correspondente a ele [Wild and Ramchandran 2005, Stevenson et al. 2009]. Por sua vez, assumimos que a localização do UP é conhecida (ex. Antena de TV), e que qualquer nó estático $n_i \in N_{SL}$ pode conhecer a distância $d_{UP}^{n_i}(t)$ a partir de UP. Assim, com base nesses dados e

considerando que as limitações físicas de um atacante (e.g. bateria, antena) forçam-no a transmitir numa potência várias ordens de magnitude menor que a do UP, o modelo de propagação de rádio (Eq. 3) e medições em n_i podem aumentar a capacidade de diferenciação entre uma transmissão primária e uma transmissão mal intencionada e melhorar a probabilidade de detectar a presença do ataque EUP. Nossas simulações foram realizadas no NS-2.31 utilizando o módulo de redes ad hoc de rádio cognitivo desenvolvido por Di Felice et al. [Felice et al. 2011], seguindo os parâmetros descritos na Tabela 2. Os valores dos parâmetros utilizados na simulação foram escolhidos considerando situações realísticas de uma CRAHN, ex. a potência de transmissão de um UP ou de um US. Além disso, configuramos 50 nós estáticos (sem mobilidade) para ver seu comportamento em situações onde a taxa de atacantes muda de forma considerável.

Tabela 2. Valores dos parâmetros de simulação

Parâmetro de simulação	Valor
Usuários secundários (USs)	50
Usuários primários (UPs)	2
Taxa de ataques EUPs	10%, 30%, 50%
Número de canais	11
Tempo de simulação	500 segundos
Área de cobertura de transmissão US	250 m
Área de cobertura de transmissão UP	1000 m
Área de cobertura de transmissão ataque EUP	250 até 1000 m
Potência de transmissão US	24.5 dBm
Potência de transmissão UP	94 dBm (conforme [Stevenson et al. 2009])
Potência de transmissão ataque EUP	24.5 to 94 dBm
Protocolo de roteamento	AODV
Área	1000x1000 m^2

A principal métrica de avaliação empregada é a **probabilidade da presença do ataque EUP** detectada por um US. Esta determina a probabilidade de sucesso do ataque a partir do momento que este é lançado na rede. Esta métrica é calculada a partir do teorema Bayesiano (Eq. 1) considerando a probabilidade preliminar do nó detector $P_{n_i}(A)$ e o conjunto de probabilidades preliminares calculadas e recebidas por cada um dos vizinhos cooperadores.

Nós também analisamos o impacto do número de vizinhos k em $P_{n_i}(A|B)$. Para isto, nós forçamos a variação de valor k em 3, 6 e 10, para realizar um cálculo da probabilidade da presença do ataque EUP limitando a quantidade de vizinhos cooperadores, para determinar a inferência que as probabilidades vizinhos dos nós causam na probabilidade inicial do nó. Esta variação da métrica principal foi chamada de **taxa de detecção** $T_{k,i}$ do nó $n_i \in N_{SL}$ diante de diferentes números de vizinhos cooperadores k. $T_{k,i}$ é dado por $T_{n_i} = \frac{\sum_{j=1}^{k} P_{n_j}(B)}{k}$, em que $P_{n_j}(B)$ é a probabilidade preliminar compartilhada pelo j-ésimo vizinho de n_i e $0 \leq k \leq |N_{SL}| - |\{n_i\}|$ é o correspondente total dos nós vizinhos cooperadores.

5.2. Resultados

Nesta subseção, nós reportamos os resultados do desempenho do INCA usando múltiplos critérios e comparamos com uma versão usando apenas o critério de potência do sinal recebido, que é o critério amplamente utilizado no estado da arte. Esta versão com um

único critério é referenciada como esquema **monocritério** nos gráficos. Nós inicialmente mostramos os resultados considerando INCA sem cooperação, ou seja, a fase individual utilizando *múltiplos critérios* frente à versão monocritério não cooperativa, para depois apresentar os resultados obtidos aplicando as duas fases do INCA. Cabe ressaltar que os resultados obtidos refletem a media de 35 simulações por cada cenário, com um intervalo de confiança de 95%.

A Figura 5 apresenta a comparação da probabilidade da presença do ataque EUP dada pela versão monocritério com as probabilidades dadas pela fase individual do INCA (isto é, a probabilidade preliminar obtida a partir de múltiplos critérios). Pode-se observar que o desempenho do esquema monocritério é levemente comprometido conforme a taxa de atacantes aumenta na rede. Estas probabilidades representam 35.96%, 35.30% e 34.48% para determinar a presença do ataque EUP com taxas de 10%, 30% e 50% de USs maliciosos nos diferentes cenários. Nestes mesmos cenários, o esquema INCA em sua fase individual com análise de múltiplos critérios supera as probabilidades de um único critério em até um 2.36%. Tais melhoras resultam do uso do NWAUF como técnica de agregação dos múltiplos critérios na primeira fase do INCA, sem considerar a fase cooperativa do esquema.

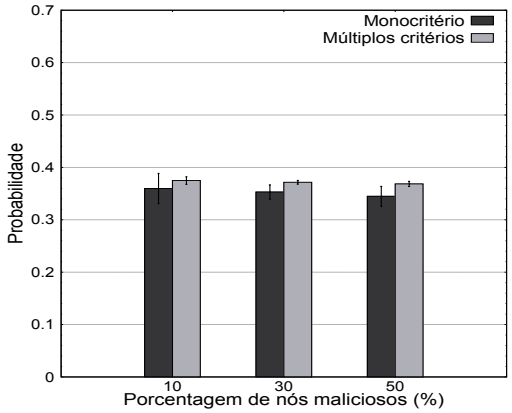

Figura 5. Fase individual do INCA vs. esquema monocritério não-cooperativo

Por sua vez, quando a probabilidade da presença do ataque EUP executa a fase de cooperação do INCA, os resultados mostram que ao comparar com o esquema monocritério cooperativo, os resultados são melhores (15.56%), como é observado na Figura 6. Desta vez, a cooperação funciona para enriquecer a análise de detecção e proporcionar uma melhoria de 12.6% em relação ao INCA em sua fase individual. Apesar disto, os benefícios obtidos pelo uso de cooperação podem ser prejudicados se uma abordagem de múltiplos critérios não acontece. Isto é fundamentado pelo fato de que um esquema monocritério cooperativo consegue 0.02% de melhoria em relação ao esquema monocritério não-cooperativo.

Finalmente, a Figura 7 compara a taxa de detecção $T_{k,i}$ sob a variação no número de vizinhos cooperadores k considerando ambos esquemas (INCA e monocritério). Na avaliação cooperativa, nós levamos em conta a quantidade de nós cooperativos e a percentagem de atacantes na CRAHN. O esquema de um único critério apresenta uma variação de 1.33% da probabilidade em cenários com 3, 6 e 10 nós cooperativos. Por sua vez, INCA apresenta uma variação de 0.3% entre os cenários com diferentes quantidades de

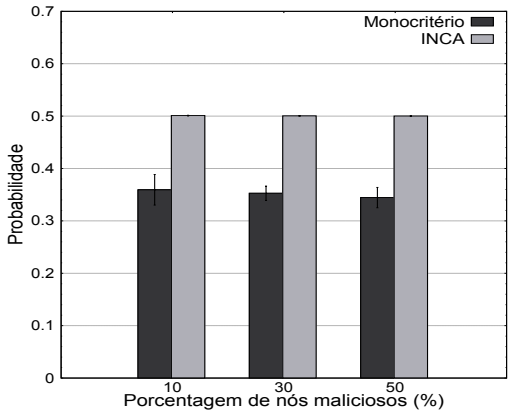

Figura 6. Esquema INCA vs esquema monocritério cooperativo

nós cooperativos. Além disso, nós verificamos que a baixa variação na probabilidade é devido ao acesso aleatório do ataque EUP, isto é um US pode não necessariamente realizar um sensoreamento do canal atacado.

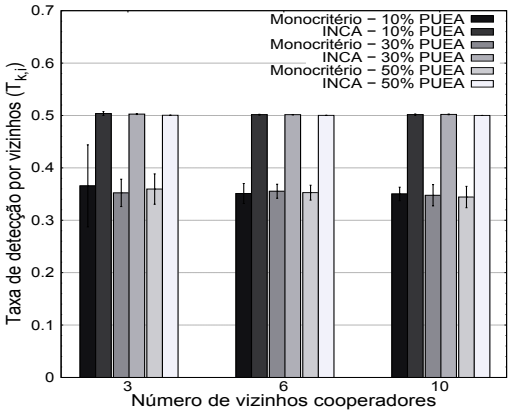

Figura 7. Taxa de detecção por números de vizinhos

6. Conclusões e trabalhos futuros

Neste trabalho, apresentamos INCA, um novo esquema de múltiplos critérios para a análise cooperativa da presença de ataques EUPs nas CRAHNs. O esquema INCA não só engloba abordagens do estado da arte, como a descentralização e a cooperação, mas também uma abordagem inovadora para levar em conta múltiplos critérios no processo de detecção de ataque EUPs. Nós comparamos os resultados gerados a partir do INCA com uma versão de um esquema que considera um único critério como forma de representar a abordagem considerada no estado da arte. Os resultados obtidos mostram que o esquema INCA tendo como base critérios adicionais, tais como a distância e a potência de transmissão, além da potência de recepção, apresenta um melhor desempenho em relação ao esquema monocritério. Cabe destacar que o esquema $INCA$ não foca seu estudo nos diferentes tipos de critérios utilizados, mas este afere que a utilização de múltiplos critérios em conjunto com uma abordagem cooperativa permite determinar uma melhor detecção da presença do ataque EUP nas redes ad hoc de rádio cognitivo.

Assim, nossos resultados indicam as vantagens de criar esquemas de detecção de ataques EUPs que incorporam múltiplos critérios para analisar os ataques de emulação de usuário primário. Uma questão importante inerente à análise de ataque EUP baseada em múltiplos critérios, como o esquema INCA, é a tarefa de atribuição de pesos para representar a importância e diferenciação dos critérios. Para os critérios considerados no estudo de caso deste trabalho, identificamos (por meio de simulações piloto *off-line*) pelo menos uma configuração de pesos que demonstrou a melhoria alcançada pela abordagem de múltiplos critérios proposta frente à abordagem representante do estado da arte. Tal resultado não somente constitui um argumento científico a favor da abordagem proposta como também cria oportunidades para trabalhos futuros. Neste sentido, um trabalho futuro poderia investigar algoritmos de otimização para a definir os pesos de forma *on-line* e variável ao longo do tempo. Adicionalmente, o impacto da mobilidade dos nós poderia ser considerada no processo de cálculo das estimativas de ataque.

Referências

Akyildiz, I., Lee, W.-Y., Vuran, M., and Mohanty, S. (2008). A survey on spectrum management in cognitive radio networks. *IEEE Comm. Mag.*, 46(4):40 –48.

Akyildiz, I. F., Lee, W.-Y., and Chowdhury, K. R. (2009). Crahns: Cognitive radio ad hoc networks. *Ad Hoc Networks*, 7(5):810–836.

Anand, S., Jin, Z., and Subbalakshmi, K. (2008). An analytical model for primary user emulation attacks in cognitive radio networks. In *IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, DySPAN*, pages 1–6.

Arianandа, D., Lakshmanan, M., and Nikoo, H. (2009). A survey on spectrum sensing techniques for cognitive radio. In *Cognitive Radio and Advanced Spectrum Management, CogART. Second International Workshop on*, pages 74 –79.

Benayoun, R., Roy, B., and Sussman, N. (1966). Manual de reference du programme electre. *Note De Synthese et Formaton, 25*.

Chen, C., Cheng, H., and Yao, Y.-D. (2011). Cooperative spectrum sensing in cognitive radio networks in the presence of the primary user emulation attack. *IEEE Trans. on Wireless Comm.*, 10(7):2135 –2141.

Chen, R. and Park, J.-M. (2006). Ensuring trustworthy spectrum sensing in cognitive radio networks. In *IEEE SDR*, pages 110 –119.

Chen, R., Park, J.-M., and Reed, J. (2008). Defense against primary user emulation attacks in cognitive radio networks. *IEEE Journal on Selected Areas in Comm.*, 26(1):25–37.

Felice, M. D., Chowdhury, K., Kim, W., Kassler, A., and Bononi, L. (2011). End-to-end protocols for cognitive radio ad hoc networks: An evaluation study. *Performance Evaluation*, 68(9):859 – 875.

Fragkiadakis, A., Tragos, E., and Askoxylakis, I. (2012). A survey on security threats and detection techniques in cognitive radio networks. *IEEE Communications Surveys Tutorials*, PP(99):1 – 18.

Jin, Z., Anand, S., and Subbalakshmi, K. (2010). Robust spectrum decision protocol against primary user emulation attacks in dynamic spectrum access networks. In *IEEE GLOBECOM*, pages 1–5.

Jin, Z., Anand, S., and Subbalakshmi, K. P. (2009). Detecting primary user emulation attacks in dynamic spectrum access networks. In *IEEE ICC*, pages 2749–2753.

Lee, W.-Y. and Akyldiz, I. F. (2011). A spectrum decision framework for cognitive radio networks. *IEEE Trans. on Mobile Computing*, 10(2):161 –174.

Li, H. and Han, Z. (2010). Dogfight in spectrum: Combating primary user emulation attacks in cognitive radio systems, part i: Known channel statistics. *IEEE Trans. on Wireless Comm.*, 9(11):3566 –3577.

Malakooti, B., Thomas, I., Tanguturi, S., Gajurel, S., and Kim, H. (2006). Multiple criteria network routing with simulation results. *Industrial Engineering Research Conference (IERC)*.

Min, A., Kim, K.-H., and Shin, K. (2011). Robust cooperative sensing via state estimation in cognitive radio networks. In *IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, DySPAN*, pages 185 –196.

Mitola, J. and Maguire, G. Q. (1999). Cognitive radio: making software radios more personal. *IEEE Pers. Comm.*, 6(4):13–18.

Saaty, T. L. (1980). The analytic hierarchy process. *McGraw Hill*.

Stevenson, C., Chouinard, G., Lei, Z., Hu, W., Shellhammer, S., and Caldwell, W. (2009). Ieee 802.22: The first cognitive radio wireless regional area network standard. *IEEE Communications Magazine*, 47(1):130 –138.

Subhedar, M. and Birajdar, G. (2011). Spectrum sensing techniques in cognitive radio networks: A survey. *International Journal of NextGeneration Networks*, 3(2):37–51.

Tan, Y., Hong, K., Sengupta, S., and Subbalakshmi, K. P. (2011). Using sybil identities for primary user emulation and byzantine attacks in DSA networks. In *IEEE GLOBECOM*, pages 1–5.

Wang, X. and Triantaphyllou, E. (2008). Ranking irregularities when evaluating alternatives by using some electre methods. *Omega*, 36(1):45 – 63.

Wild, B. and Ramchandran, K. (2005). Detecting primary receivers for cognitive radio applications. In *IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, DySPAN*, pages 124 –130.

Yuan, Z., Niyato, D., Li, H., and Han, Z. (2011). Defense against primary user emulation attacks using belief propagation of location information in cognitive radio networks. In *IEEE Wireless Communications and Networking Conference (WCNC)*, pages 599 – 604.

Z. Jin, S. A. and Subbalakshmi, K. P. (2010). Neat: A neighbor assisted spectrum decision protocol for resilience against primary user emulation attacks. Technical report, Department of Electrical and Computer Engineering, Stevens Institute of Technology, Hoboken, NJ.

Zhang, W., Mallik, R., and Letaief, K. (2009). Optimization of cooperative spectrum sensing with energy detection in cognitive radio networks. *IEEE Transactions on Wireless Communications*, 8(12):5761 –5766.

